## REMARKS/ARGUMENTS

Claims 24-39 are pending in the present application. Claims 1-23 are canceled. Support for the new claims can be found in the Specification on page 11, lines 18-32; pages 12, 15, and 16. No new matter is added by any of the amendments. Consideration of the claims is respectfully requested.

### I. 35 U.S.C. § 101

The Examiner rejects claims 15-21 under 35 U.S.C. § 101 as being directed towards non-statutory subject matter. Applicants have canceled claim 15-23. Therefore, the rejection with respect to these claims is moot. New claims 34 and 38 incorporate language, suggested by the Examiner in the Final Office action of June 28, 2007. Claims 34 and 38 recite a computer program product ***stored in a computer readable medium.***

### II. 35 U.S.C. § 102, Anticipation

The Examiner rejects claims 1, 3, 4, 5, 11, 12, 15, and 17-19 under 35 U.S.C. § 102 as being anticipated by Jin et al. (U.S. 6,311,275) (hereinafter "*Jin*"). Claims 1-23 are canceled. Therefore, with respect to these claims this rejection is moot. However, newly added claims 24-39 recite some subject matter addressed by the Examiner in the rejection of claims 1, 3, 4, 5, 11, 12, 15, and 17-19 under 35 U.S.C. § 102. Regarding claim 1 the Examiner states:

> As per claim 1, Jin et al teaches of a method in a data processing system for providing addresses to clients, the method comprising receiving a request from a client for an address; determining whether authentication information is present in the request; performing an authentication process using the authentication information if the authentication information is presenting the request; determining whether the authentication information is authenticated; and responsive to the authentication information being authenticated, providing a privileged address to the client and responsive to the authentication information not being authenticated, providing a dummy (standard) address to the client

Final Office Action of June 28, 2007, page 5.

Claim 24 is as follows:

> 24. (New) A computer implemented method in a data processing system for providing addresses to clients, the computer implemented method comprising:
>
> receiving a request from a client for an address, wherein the request comprises a unique client identifier and authentication information, and wherein the authentication information comprises at least one of a pass phrase and a digital certificate;
>
> determining whether the authentication information is present in the request;
>
> responsive to determining that the authentication information is present in the request, performing a verification process on the authentication information to authenticate the request;

responsive to authenticating the request, checking a privileged address table to determine whether an privileged address is assigned to the client forming a previously assigned privileged address, wherein the privileged address is a static internet protocol address in a pool of privileged addresses stored in a memory of a data processing system;

responsive to determining that the privileged address is assigned to the client, assigning the previously assigned privileged address to the client to form a previously assigned privileged address and sending an offer to the client, wherein the offer comprises the previously assigned privileged address and the authentication information; and

responsive to determining that the privileged address is not assigned to the client, assigning a unassigned privileged address, from the pool of privileged addresses, to the client to form an assigned privileged address and sending the offer to the client, wherein the offer comprises the assigned privileged address and the authentication information

*Jin* fails to teach "responsive to authenticating the request to form an authenticated request, providing a privileged address to the client, wherein the privileged address is a static internet protocol address in a set of privileged addresses stored in a memory of a data processing system," as is recited in claim 24. In rejecting claim 1 the Examiner cites to the following portion of *Jin:*

As described above, the user initiates a session on the network 5 by launching a dial-up application on his or her subscriber PC 1. The dial-up application prompts the user for user-name and password information, and contacts the NAS 2. The NAS 2 prepares an access-request packet containing the user-specified information, as well as information about the NAS client 2 itself. Instead of being delivered directly to the AAA Server 4, however, the access-request packet is first intercepted by the SSG Server 3, at step 200. Since the access-request packet contains username and password information, receipt of the access-request packet by the SSG Server 3 supplants the need for requiring the user to supply this information to the SSG Server 3 using a separate dashboard application. However, as described above, the SSG Server 3 still needs the user IP address to complete the log-on procedure. The user IP address, however, has not yet been assigned, and extra steps must be taken before the SSG Server 3 can officially log the user on.

The SSG Server 3 forwards the access-request packet to the AAA Server 4 at step 202. The AAA Server 4 first authenticates the user by checking the data attributes in the access-request packet against its account database. The AAA Server 4 then responds to the access-request by issuing an access-reply packet back to the SSG Server 3 at step 204. If the user authentication check is successful, then the AAA Server 4 may assign an IP address to the user and include this IP address in the access-reply packet. The SSG server 3 then checks for an IP address in the access-reply packet. If the SSG Server 3 finds an IP address, then the SSG Server 3 can log the user on with the IP address provided by the AAA Server 4, and then forward the access-reply packet on to the NAS 2 immediately at step 206. Once the access-reply packet is received by the NAS 2, it may then log the user on as well, and the user session can begin.

If the AAA Server 4 authorizes the user but does not assign an IP address, then the SSG Server 3 can log the user on with a dummy temporary IP address. It then assigns the user an identification number that it inserts into the access-reply packet before forwarding the access-reply packet to the NAS 2 at step 206. The identification number is written as a special attribute in the access-reply packet, called a "class attribute" in the RADIUS protocol. The class attribute is read and stored by the NAS 2 and echoed back

> unchanged in subsequent packets. The temporary IP address can be used as an identification number.
>
> Upon receipt of the access-reply packet authorizing the user to access the network, the NAS 2 assigns a genuine IP address to the user and logs the user on.

*Jin*, col, 4, line 44 – col. 5, line 10-24.

*Jin* describes a method of providing a single step log-on access for a subscriber to a computer network. *Jin* teaches that when a user initiates a session on the network, the network access server (NAS) prepares an access-request packet that contains user-specified information and information regarding the NAS client. After an IP address has been supplied by the SSG Server, and upon receipt of the access-reply packet authorizing the user to access the network, the NAS assigns a genuine IP address to the user and logs the user on. However, *Jin* does not teach any type of ***privileged address*** as claimed in claim 24. *Jin* provides a genuine address, which is not the same as a static internet protocol address in a set of privileged addresses stored in a memory of a data processing system, claimed in claim 24. Therefore each and every element recited in claim 24 is not identically shown in *Jin*. Accordingly, claim 24 is not anticipated by the cited reference.

Newly added independent claims 28, 29, 33, 34, 38, and 39 recite some similar subject matter that is discussed above with regard to claim 24. Therefore, independent claims 28, 29, 33, 34, 38, and 39 are not anticipated *Jin* for at least the reasons set forth above with regard to the similarly recited subject matter.

Dependent claims 25-27, 30-32, and 35-37 depend from claims 28, 29, 33, 34, 38, and 39. Therefore, at least by virtue of their dependency, dependent claims 25-27, 30-32, and 35-37 are not anticipated by *Jin*.

## III. 35 U.S.C. § 103, Obviousness

### III.A. Claims 6, 13, and 20

The Examiner rejects claims 6, 13, and 20 under 35 U.S.C. § 103 as being unpatentable over *Jin*. Applicants have canceled claims 6, 13, and 20. Therefore the rejection with respect to these claims is moot.

### III.B. Claims 7, 14, and 21

The Examiner also rejects claims 7, 14, and 21 under 35 U.S.C. § 103 as obvious over Droms, Dynamic Host Configuration Protocol, Request For Comments: 2131, March 1997 (hereinafter "*Droms RFC 2131*") in view of Droms, Authentication for DHCP Messages, Request For Comments: 3118, June

2001 (hereinafter "*Droms RFC 3118*"). Applicants have canceled claims 7, 14, 21. Therefore, the rejection with respect to these claims is moot.

Newly added claims 28, 33, and 38 recite some subject matter addressed by the Examiner in the rejection of claims 7, 14, and 21. Claim 28 is as follows:

> 28. (New) A computer implemented method in a data processing system for assigning addresses to clients, the computer implemented method comprising:
> sending a request for a privileged address to a server from a client, wherein the request comprises a unique client identifier and authentication information, and wherein the authentication information comprises at least one of a pass phrase and a digital certificate, wherein the server performs a verification process on the authentication information to authenticate the request, and wherein the privileged address is a static internet protocol address in a pool of privileged addresses;
> receiving an offer from the server, wherein the offer comprises a privileged address and authentication information;
> determining whether the offer is authentic; and
> responsive to determining that the offer is authentic, accepting the offer.

Regarding claim 7 the Examiner states:

> As per claims 7,14, and 21, it is taught by Droms, RFC 2131 of a receiving a request from a client for an address; determining whether information is present in the request; performing a verification process using the information if the information is present in the request; determining whether the information is verified; responsive to the information being verified, providing an address to the client; responsive to the information not being verified, denying the request receiving the address by the client, wherein the address received by the client is included in an offer from a server that performed the verification process; determining, by the client, whether the offer is valid; and responsive to the offer being valid, accepting the offer by the client (section 3.1, page 13 and steps 3-5 on pages 15-16). The teachings of Droms, RFC 2131 fail to disclose of using authentication information to be authenticate the DHCP communications between the server and the client. In an expanded teaching of Drorns, RFC 21 31, Droms et all RFC 31 18 discloses that authentication occurs between a server and client in order to compl'ete the DHCP process (page 4, section 1.4, step 5; page 6, section 5.3; and page 7, section 5.5.1). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to use authentication measures in order to validate the assignment of an IP address.

Final Office Action of June28, 2007, page 8.

*Droms RFC 2131* in view of *Droms RFC 3118* does not teach or suggest "a privileged address" as recited in claim 28. The Examiner cites to *Droms RFC 2131*, section 3.1, page 13 and steps-3-5 on pages 15-16. The cited to section teaches adding the capability of automatic allocation of reusable network addresses and an additional configuration option, using BOOTP relay agents. *Droms RFC 2131* further teaches a new DHCP message type, a classing mechanism for identifying DHCP clients to DHCP servers and other editorial changes to clarify the text as a result of experience gained in DHCP interoperability tests.

However, the Examiner admits, and Applicants agree, that *Droms RFC 2131* fails to teach each and every feature of claimed invention. The Examiner cites to *Droms RFC 3118* as making up for the deficiencies of *Droms RFC 2131*. *Droms RFC 3118* states:

> If the protocol field is 1, the message is using the "delayed authentication" mechanism. In delayed authentication, the client requests authentication in its DHCPDISCOVER message and the server replies with a DHCPOFFER message that includes authentication information. This authentication information contains a nonce value generated by the source as a message authentication code (MAC) to provide message authentication and entity authentication.
>
> 5.3 Message validation
>
> To validate an incoming message, the receiver first checks that the value in the replay detection field is acceptable according to the replay detection method specified by the RDM field. Next, the receiver computes the MAC as described in [3]. The receiver MUST set the 'MAC' field of the authentication option to all 0s for computation of the MAC, and because a DHCP relay agent may alter the values of the 'giaddr' and 'hops' fields in the DHCP message, the contents of those two fields MUST also be set to zero for the computation of the MAC. If the MAC computed by the receiver does not match the MAC contained in the authentication option, the receiver MUST discard the DHCP message.
>
> 5.5.1 INIT state
>
> When in INIT state, the client uses delayed authentication as follows:
>
> 1. The client MUST include the authentication request option in its DHCPDISCOVER message along with a client identifier option [6] to identify itself uniquely to the server.
>
> 2. The client MUST perform the validation test described in section 5.3 on any DHCPOFFER messages that include authentication information. If one or more DHCPOFFER messages pass the validation test, the client chooses one of the offered configurations.
>
> Client behavior if no DHCPOFFER messages include authentication information or pass the validation test is controlled by local policy in the client. According to client policy, the client MAY choose to respond to a DHCPOFFER message that has not been authenticated.

*Droms RFC 3118*, page 4, section 1.4, step 5; page 6, section 5.3; and page 7, section 5.5.1.

*Droms RFC 3118* teaches a method for authenticating DHCP Messages using a specific format option, i.e. a request. The format option comprises the following fields: an authentication code, which is assigned a value of 90, a protocol length, a protocol, an algorithm, a RDM, a Replay Detection, and authentication information. The architecture of the request in *Droms RFC 3118* is clearly unlike the request as claim in claim 24. The request of the claimed invention comprises a unique identifier and the authentication information. However, *Droms RFC 3118* fails to make up for the deficiencies in *Droms RFC 2131,* because one of ordinary skill in the art would not modify the invention in *Droms RFC 3118* to accommodate the request in the claimed invention, because the claimed request would not be operable in *Droms RFC 3118*. The claimed request would not be operable in *Droms RFC 3118* because of the lack of the other required request fields recited in *Droms RFC 3118*.

Additionally, nothing in *Droms RFC 3118* teaches ". . . providing a privileged address to the client, wherein the privileged address is one of the ones of static internet protocol address in a set of privileged addresses stored in a memory of a data processing system." Therefore, the proposed combinations of *Droms RFC 2131* and *Droms RFC 3118,* considered as a whole, fails to teach or suggest the each and every feature of claim 24. Accordingly, a rejection under 35 U.S.C. § 103 is overcome.

Newly added independent claims 33 and 38 recite some similar subject matter that is discussed above with regard to claim 28. Therefore, independent claims 33 and 38 are not obvious for at least the reasons set forth above with regard to the similarly recited subject matter.

### III.C. Claims 8, 9, 22

The Examiner rejects claims 8, 9, and 22 under 35 U.S.C. § 103 as obvious over *Jin* in view of Bahl et al. (U.S. 6,957,276) (hereinafter "*Bahl*"). Applicants have canceled claims 8, 9, 22. Therefore, the rejection with respect to these claims is moot.

Newly added claims 29, 30, and 39 recite some subject matter addressed by the Examiner in the rejection of claims 8, 9, and 22. Claim 29 is as follows:

> 29. (New) A data processing system for providing addresses to clients, the data processing system comprising:
>
> receiving means for receiving a request from a client for an address, wherein the request comprises a unique client identifier and authentication information, and wherein the authentication information comprises at least one of a pass phrase and a digital certificate;
>
> determining means for determining whether the authentication information is present in the request;
>
> responsive to determining that the authentication information is present in the request, performing means for performing a verification process on the authentication information to authenticate the request;
>
> responsive to authenticating the request, checking means for checking a privileged address table to determine whether an privileged address is assigned to the

client forming a previously assigned privileged address, wherein the privileged address is a static internet protocol address in a pool of privileged addresses stored in a memory of a data processing system;

responsive to determining that a privileged address is assigned to the client, assigning means for assigning the previously assigned privileged address to the client and sending means for sending an offer to the client, wherein the offer comprises the previously assigned privileged address and the authentication information; and

responsive to determining that a privileged address is not assigned to the client, assigning means for assigning the privileged address from the pool of privileged addresses, to the client and sending means for sending an offer to the client, wherein the offer comprises the privileged address and the authentication information.

Regarding claim 8 the Examiner states:

As per claim 8, it is disclosed by Jin et al of a data processing system for providing addresses to clients, the data processing system comprising receiving means for receiving a request from a client for an address; first determining means for determining whether authentication information is present in the request; performing means for performing an authentication process using the authentication information if the authentication information is presenting the request; second determining means for determining whether the authentication information is authenticated; and providing means, responsive to the authentication information being authenticated, for providing aprivileged address to the client (col. 4, line 44 through col. 5, line 10 and col. 5, lines 22-24). The teachings of Jin et al fail to disclose that the privileged address is a static IP address that is identical to a previous address that was provided to a client. It is taught by Bahl et al that the privileged address is a static IP address that is identical to a previous address that was provided to a client (col. 2, lines 57 through col. 3, line 7). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to reclaim static addresses. The teachings of Bahl et al discloses of motivation for static IP address being is identical to a previous address that was provided to a client by reciting of an automated approach so that the assignment of static addresses can be done in a centralized manner so that an administrator doesn't have to physically visit each machine to make the changes (col. 2, lines 12-17 & 57-63). It is obvious that the teachings of Jin et al would have found the teachings of Bahl et al beneficial so that the same static addresses can be assigned in a centralized manner.

As per claim 9, Jin et al teaches of further comprising providing means, responsive to the authentication information not being authenticated, for providing a standard address to the client (col. 5, lines 11-21).

As per claim 22, Jin et al discloses of a data processing system for providing addresses to clients, the data processing system comprising a bus system; a memory connected to the bus system, wherein the memory includes a set of instructions; a communications adaptor connected to the bus system; and a processor unit connected to the bus system, wherein the processor unit-executes the set of instructions to receive a request from a client for an address; determine whether authentication information is present in the request; perform an authentication process using the authentication information if the authentication information is presenting the request; determine

whether the authentication information is authenticated; and provide a privileged address to the client in response to the authentication information being authenticated (col. 4, line **44** through col. 5, line 10 and col. 5, lines 22-24).

Final Office Action of June 28, 2007, pages 9-11.

The Examiner failed to state a prima facie obviousness rejection against these claims because the proposed combination of *Jin* in view of *Bahl*, considered as a whole, does not teach or suggest the features of the claimed invention because no proper reason exists under *KSR Int'l.* to combine the references. No proper reason exists to combine the references exists because both *Jin* and *Bahl* represent complete solutions to the problems each solves. *Jin* describes a method of providing a single step log-on access for a subscriber to a computer network wherein a genuine address is provided. This genuine address is not the same as the privileged address claimed in claim 24.

*Bahl* is directed to a method and system for assigning and reclaiming static IP addresses using a DHCP server. See *Bahl* col. 2 lines 57 – col. 3, lines 1-46. *Bahl* teaches that when a client machine boots or resumes the IP address is checked to see if the IP address is associated with a remove flag. If this flag is set the client enters the initialization state to discover a new IP address. When the flag is not set, the client enters the initialization reboot state to renew the old IP address.

Neither *Jin* nor *Bahl* teaches or suggest all the claim features of claimed invention. Moreover, each reference provides a complete solution to the problem that each reference represents. One of ordinary skill in the art would see no benefit to combining the references. Therefore, one of ordinary skill would have no reason to combine or otherwise modify the references. For this reason, no proper reason exists under *KSR Int'l.* to combine the references to achieve the invention as claimed.

Newly added independent claims 39 recite some similar subject matter that is discussed above with regard to claim 29. Therefore, independent claim 39 is not obvious over *Jin* in view of *Bahl* for at least the reasons set forth above with regard to the similarly recited subject matter.

Dependent claims 30-32 depend from claim 29. Therefore, at least by virtue of their dependency, dependent claims 30-32 are not obvious over *Jin* in view of *Bahl*.

## IV. Conclusion

It is respectfully urged that the subject application is patentable over the cited references and is now in condition for allowance.

The examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: April 29, 2008

Respectfully submitted,

/LaRhonda Jefferson-Mills/

LaRhonda Jefferson-Mills
Reg. No. 61,649
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorney for Applicants